

# Release Notes

## FortiAnalyzer 7.0.0



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/support-and-training/training.html>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



July 9, 2021

FortiAnalyzer 7.0.0 Release Notes

05-700-690786-20210709

# TABLE OF CONTENTS

<b>Change Log</b>	<b>5</b>
<b>FortiAnalyzer 7.0.0 Release</b>	<b>6</b>
Supported models	6
FortiAnalyzer VM subscription license	6
Management extension applications	7
Supported models for MEA	7
Minimum system requirements	7
FortiRecorder	8
Supported models for FortiRecorder	8
Supported cameras	8
<b>Special Notices</b>	<b>9</b>
Citrix XenServer default limits and upgrade	9
FortiAnalyzer VM upgrade requires more memory	9
Maximum ADOM limits for FortiAnalyzer	9
Port 8443 reserved	10
Hyper-V FortiAnalyzer-VM running on an AMD CPU	10
SSLv3 on FortiAnalyzer-VM64-AWS	10
<b>Upgrade Information</b>	<b>11</b>
Downgrading to previous versions	11
Firmware image checksums	11
FortiAnalyzer VM firmware	11
SNMP MIB files	13
<b>Product Integration and Support</b>	<b>14</b>
FortiAnalyzer version 7.0.0 support	14
Web browsers	14
FortiOS/FortiOS Carrier	15
FortiADC	15
FortiAnalyzer	15
FortiAuthenticator	15
FortiCache	15
FortiClient	16
FortiDDoS	16
FortiDeceptor	16
FortiMail	16
FortiManager	17
FortiNAC	17
FortiProxy	17
FortiSandbox	17
FortiSwitch ATCA	17
FortiWeb	18
Virtualization	18
Feature support	18
Language support	19

---

Supported models .....	20
FortiGate models .....	21
FortiCarrier models .....	25
FortiADC models .....	26
FortiAnalyzer models .....	27
FortiAuthenticator models .....	28
FortiCache models .....	28
FortiDDoS models .....	28
FortiDeceptor models .....	28
FortiMail models .....	28
FortiNAC models .....	29
FortiProxy models .....	29
FortiSandbox models .....	29
FortiSwitch ATCA models .....	30
FortiWeb models .....	30
<b>Resolved Issues .....</b>	<b>33</b>
Device Manager .....	33
Fabric View .....	33
FortiSOC .....	33
FortiView .....	33
Log View .....	34
Others .....	35
Reports .....	36
System Settings .....	36
<b>Known Issues .....</b>	<b>38</b>
Device Manager .....	38
Event Management .....	38
FortiView .....	38
Log View .....	39
Others .....	40
Reports .....	40
System Settings .....	40
<b>Appendix A - Default and maximum number of ADOMs supported .....</b>	<b>41</b>
Hardware models .....	41
Virtual Machines .....	41

# Change Log

Date	Change Description
2021-04-22	Initial release of 7.0.0.
2021-04-23	Updated supported models to remove old, unsupported versions.
2021-06-10	Added 724625 to <a href="#">Known Issues on page 38</a> and updated <a href="#">Upgrade Information on page 11</a> .
2021-06-21	Updated <a href="#">Resolved Issues on page 33</a> .
2021-06-28	Added note about ports to <a href="#">Management extension applications on page 7</a> .
2021-07-09	Added support for FortiSandbox 4.0 to <a href="#">FortiSandbox on page 17</a> and <a href="#">FortiSandbox models on page 29</a> .

# FortiAnalyzer 7.0.0 Release

This document provides information about FortiAnalyzer version 7.0.0 build 0047.



The recommended minimum screen resolution for the FortiAnalyzer GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

This section includes the following topics:

- [Supported models on page 6](#)
- [FortiAnalyzer VM subscription license on page 6](#)
- [Management extension applications on page 7](#)
- [FortiRecorder on page 8](#)

## Supported models

FortiAnalyzer version 7.0.0 supports the following models:

<b>FortiAnalyzer</b>	FAZ-150G, FAZ-300F, FAZ-300G, FAZ-400E, FAZ-800F, FAZ-1000F, FAZ-2000E, FAZ-3000F, FAZ-3000G, FAZ-3500E, FAZ-3500F, FAZ-3500G, FAZ-3700F, FAZ-3900E
<b>FortiAnalyzer VM</b>	FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-GCP, FAZ-VM64-HV (including Hyper-V 2016, 2019), FAZ-VM64-KVM, FAZ-VM64-OPC, FAZ-VM64-Xen (for both Citrix and Open Source Xen)

## FortiAnalyzer VM subscription license

The FortiAnalyzer VM subscription license supports FortiAnalyzer version 6.4.1 and later. For information about supported firmware, see [FortiAnalyzer VM firmware on page 11](#).

See also [Appendix A - Default and maximum number of ADOMs supported on page 41](#).



You can use the FortiAnalyzer VM subscription license with new FAZ-VM installations. For existing FAZ-VM installations, you cannot upgrade to a FortiAnalyzer VM subscription license. Instead, you must migrate data from the existing FAZ-VM to a new FAZ-VM with subscription license.

## Management extension applications

The following section describes supported models and minimum system requirements for management extension applications (MEA) in FortiAnalyzer 7.0.0.



FortiAnalyzer uses port TCP/443 or TCP/4443 to connect to the Fortinet registry and download MEAs. Ensure that the port is also open on any upstream FortiGates. For more information about incoming and outgoing ports, see the [FortiAnalyzer 7.0 Ports Guide](#).

### Supported models for MEA

You can use any of the following FortiAnalyzer models as a host for management extension applications:

<b>FortiAnalyzer</b>	FAZ-3000F, FAZ-3000G, FAZ-3500E, FAZ-3500F, FAZ-3500G, FAZ-3700F, FAZ-3900E
<b>FortiAnalyzer VM</b>	FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-GCP, FAZ-VM64-HV (including Hyper-V 2016, 2019), FAZ-VM64-KVM, FAZ-VM64-OPC, FAZ-VM64-Xen (for both Citrix and Open Source Xen)

### Minimum system requirements

By default FortiAnalyzer VMs use the following system resource settings:

- 4 vCPU
- 8 GB RAM
- 500 GB disk space

Starting with FortiAnalyzer 7.0.0, RAM and CPU is capped at 50% for MEAs. (Use the `config system docker` command to view the setting.) If FortiAnalyzer has 8 CPUs and 16 GB RAM, then only 4 CPUs and 8 GB RAM are available to MEAs by default, and the 4 CPUs and 8 GB RAM are used for all enabled MEAs.

Some MEAs have minimum system requirements that require you to increase system resources. The following table identifies the minimum requirements for each MEA as well as the recommended system resources to function well in a production environment.

MEA minimum system requirements apply only to the individual MEA and do not take into consideration any system requirements for resource-sensitive FortiAnalyzer features or multiple, enabled MEAs.

Management Extension Application	Minimum system requirements	Recommended system resources for production*
<b>FortiSOAR</b>	<ul style="list-style-type: none"> <li>• 4 vCPU</li> <li>• 8 GB RAM</li> <li>• 500 GB disk storage</li> </ul>	<ul style="list-style-type: none"> <li>• 16 vCPU</li> <li>• 64 GB RAM</li> <li>• No change for disk storage</li> </ul>

\*The numbers in the *Recommended system resources for production* column are a combination of the default system resource settings for FortiAnalyzer plus the minimum system requirements for FortiSOAR.

## FortiRecorder

This section identifies what FortiAnalyzer models support the FortiRecorder module and what FortiCamera models are supported.

### Supported models for FortiRecorder

Below is a list of the FortiAnalyzer appliances that support the FortiRecorder module.

Platform	Maximum number of cameras
FAZ-300F	6
FAZ-400E	12
FAZ-800F	16
FAZ-1000F	50
FAZ-2000E	40
FAZ-3000F	50
FAZ-3500G	50
FAZ-3700F	60

### Supported cameras

The FortiRecorder module supports the following FortiCamera models:

- FCM-CB20
- FCM-FD20
- FCM-FD20B
- FCM-FD40
- FCM-MB40
- FCM-MD20
- FCM-MD40
- FCM-OB30



# Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer version 7.0.0.

## Citrix XenServer default limits and upgrade

Citrix XenServer limits ramdisk to 128M by default. However the FAZ-VM64-XEN image is larger than 128M. Before updating to FortiAnalyzer 6.4, increase the size of the ramdisk setting on Citrix XenServer.

### To increase the size of the ramdisk setting:

1. On Citrix XenServer, run the following command:  

```
xenstore-write /mh/limits/pv-ramdisk-max-size 536,870,912
```
2. Confirm the setting is in effect by running `xenstore-ls`.  
-----  

```
limits = ""  
pv-kernel-max-size = "33554432"  
pv-ramdisk-max-size = "536,870,912"  
boot-time = ""
```

  
-----
3. Remove the pending files left in `/run/xen/pygrub`.



The ramdisk setting returns to the default value after rebooting.

---

## FortiAnalyzer VM upgrade requires more memory

When upgrading FortiAnalyzer VM units from FortiAnalyzer 6.2.x to FortiAnalyzer 6.4.0 and later, the upgrade may fail because of memory allocation.

**Workaround:** Before upgrading FortiAnalyzer VM to FortiAnalyzer 6.4.0 and later, change the memory allocation to 8 GB of RAM.

## Maximum ADOM limits for FortiAnalyzer

FortiAnalyzer hardware devices and VMs display a warning when the maximum number of ADOMs is reached or exceeded. The platform does not enforce the limit; however, adding more ADOMs may affect the performance of the

unit. For more details, see [Appendix A - Default and maximum number of ADOMs supported on page 41](#).

## Port 8443 reserved

Port 8443 is reserved for https-logging from FortiClient EMS for Chromebooks.

## Hyper-V FortiAnalyzer-VM running on an AMD CPU

A Hyper-V FAZ-VM running on a PC with an AMD CPU may experience a kernel panic. Fortinet recommends running VMs on an Intel-based PC.

## SSLv3 on FortiAnalyzer-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiAnalyzer-VM64-AWS only enables TLSv1 by default. All other models enable both TLSv1 and SSLv3. If you wish to disable SSLv3 support, please run:

```
config system global
    set ssl-protocol tlsv1
end
```

# Upgrade Information

You can upgrade FortiAnalyzer 6.4.0 through 6.4.5 directly to 7.0.0.

Upgrade from FortiAnalyzer 6.4.6 to 7.0.0 is not supported. See 724625 in [Known Issues on page 38](#).



For other upgrade paths and details about upgrading your FortiAnalyzer, see *FortiAnalyzer Upgrade Guide*.

---

This section contains the following topics:

- [Downgrading to previous versions on page 11](#)
- [Firmware image checksums on page 11](#)
- [FortiAnalyzer VM firmware on page 11](#)
- [SNMP MIB files on page 13](#)

## Downgrading to previous versions

FortiAnalyzer does not provide a full downgrade path. You can downgrade to a previous firmware release via the GUI or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset all-settings
execute format {disk | disk-ext4}
```

## Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, <https://support.fortinet.com>. To verify the integrity of the download, select the *Checksum* link next to the *HTTPS* download link. A dialog box will be displayed with the image file name and checksum code. Compare this checksum with the checksum of the firmware image.

## FortiAnalyzer VM firmware

Fortinet provides FortiAnalyzer VM firmware images for Amazon AWS, Citrix and Open Source XenServer, Linux KVM, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

## Amazon Web Services

- The 64-bit Amazon Machine Image (AMI) is available on the AWS marketplace.

## Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains the QCOW2 file for the Open Source Xen Server.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains the Citrix XenServer Disk (VHD), and OVF files.

## Google Cloud Platform

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.out.gcp.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation.

## Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains QCOW2 that can be used by qemu.

## Microsoft Azure

The files for Microsoft Azure have AZURE in the filenames, for example `FAZ_VM64_AZURE-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.hyperv.zip`: Download the package for a new FortiAnalyzer VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Azure.

## Microsoft Hyper-V Server

The files for Microsoft Hyper-V Server have HV in the filenames, for example, `FAZ_VM64_HV-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.hyperv.zip`: Download the package for a new FortiAnalyzer VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.



Microsoft Hyper-V 2016 is supported.

---

## Oracle Private Cloud

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.out.opc.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation.

### VMware ESX/ESXi

- `.out`: Download either the 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.



For more information, see the [FortiAnalyzer Data Sheet](#) available on the Fortinet web site. VM installation guides are available in the [Fortinet Document Library](#).

---

## SNMP MIB files

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiAnalyzer v5.00 file folder.

# Product Integration and Support

This section lists FortiAnalyzer 7.0.0 support of other Fortinet products. It also identifies what FortiAnalyzer features are supported for log devices and what languages FortiAnalyzer GUI and reports support. It also lists which Fortinet models can send logs to FortiAnalyzer.

The section contains the following topics:

- [FortiAnalyzer version 7.0.0 support on page 14](#)
- [Feature support on page 18](#)
- [Language support on page 19](#)
- [Supported models on page 20](#)

## FortiAnalyzer version 7.0.0 support

This section identifies FortiAnalyzer version 7.0.0 product integration and support information:

- [Web browsers on page 14](#)
- [FortiOS/FortiOS Carrier on page 15](#)
- [FortiAnalyzer on page 15](#)
- [FortiAuthenticator on page 15](#)
- [FortiCache on page 15](#)
- [FortiClient on page 16](#)
- [FortiDDoS on page 16](#)
- [FortiDeceptor on page 16](#)
- [FortiMail on page 16](#)
- [FortiManager on page 17](#)
- [FortiNAC on page 17](#)
- [FortiProxy on page 17](#)
- [FortiSandbox on page 17](#)
- [FortiSwitch ATCA on page 17](#)
- [FortiWeb on page 18](#)
- [Virtualization on page 18](#)



Always review the Release Notes of the supported platform firmware version before upgrading your device.

---

## Web browsers

This section lists FortiAnalyzer version 7.0.0 product integration and support for web browsers:

- Microsoft Edge 80 (80.0.361 or later)
- Mozilla Firefox version 88
- Google Chrome version 90

## FortiOS/FortiOS Carrier

This section lists FortiAnalyzer version 7.0.0 product integration and support for FortiOS/FortiOS Carrier:

- 7.0.0
- 6.4.0 and later
- 6.2.0 and later
- 6.0.0 and later
- 5.6.0 and later
- 5.4.0 and later

## FortiADC

This section lists FortiAnalyzer version 7.0.0 product integration and support for FortiADC:

- 6.0.2
- 5.4.5

## FortiAnalyzer

This section lists FortiAnalyzer version 7.0.0 product integration and support for FortiAnalyzer:

- 7.0.0
- 6.4.0 and later
- 6.2.0 and later
- 6.0.0 and later
- 5.6.0 and later
- 5.4.0 and later

## FortiAuthenticator

This section lists FortiAnalyzer version 7.0.0 product integration and support for FortiAuthenticator:

- 6.0 to 6.2
- 5.0 to 5.5
- 4.3.0 and later

## FortiCache

This section lists FortiAnalyzer version 7.0.0 product integration and support for FortiCache:

- 4.2.9
- 4.1.6
- 4.0.4

## FortiClient

This section lists FortiAnalyzer version 7.0.0 product integration and support for FortiClient:

- 6.4.0 and later
- 6.2.7 and later
- 6.0.9 and later
- 5.6.6
- 5.4.0 and later

## FortiDDoS

This section lists FortiAnalyzer version 7.0.0 product integration and support for FortiDDoS:

- 5.4.3
- 5.3.1
- 5.2.0
- 5.1.1
- 5.0.0
- 4.7.0
- 4.6.0
- 4.5.0
- 4.4.2
- 4.3.2
- 4.2.3

## FortiDeceptor

This section lists FortiAnalyzer version 7.0.0 product integration and support for FortiDeceptor:

- 3.1.1

## FortiMail

This section lists FortiAnalyzer version 7.0.0 product integration and support for FortiMail:

- 6.4.3 and later
- 6.2.6
- 6.0.10 and later
- 5.4.12
- 5.3.13



## FortiManager

This section lists FortiAnalyzer version 7.0.0 product integration and support for FortiManager:

- 7.0.0
- 6.4.0 and later
- 6.2.0 and later
- 6.0.0 and later
- 5.6.0 and later
- 5.4.0 and later

## FortiNAC

This section lists FortiAnalyzer version 7.0.0 product integration and support for FortiNAC:

- 8.8.0 and later
- 8.7.0 and later
- 8.6.2 and later
- 8.5.4

## FortiProxy

This section lists FortiAnalyzer version 7.0.0 product integration and support for FortiProxy:

- 1.0 to 1.2

## FortiSandbox

This section lists FortiAnalyzer version 7.0.0 product integration and support for FortiSandbox:

- 4.0.0
- 3.2.1 and later
- 3.1.4
- 3.0.6
- 2.5.2
- 2.4.1
- 2.3.3
- 2.2.2

## FortiSwitch ATCA

This section lists FortiAnalyzer version 7.0.0 product integration and support for FortiSwitch ATCA:

- 5.0.0 and later

## FortiWeb

This section lists FortiAnalyzer version 7.0.0 product integration and support for FortiWeb:

- 6.3.0 and later
- 6.2.0 to 6.2.4
- 6.1.0 to 6.1.2
- 6.0.0 to 6.0.7
- 5.9.0 to 5.9.1
- 5.8.0 to 5.8.6
- 5.7.0 to 5.7.1
- 5.6.0 to 5.6.1
- 5.5.0 to 5.5.6
- 5.4.1 to 5.4.1

## Virtualization

This section lists FortiAnalyzer version 7.0.0 product integration and support for virtualization:

- Amazon Web Service AMI, Amazon EC2, Amazon EBS
- Citrix XenServer 7.2
- Google Cloud Platform
- Linux KVM Redhat 7.1
- Microsoft Azure
- Microsoft Hyper-V Server 2012 and 2016
- Nutanix AHV (AOS 5.10.5)
- OpenSource XenServer 4.2.5
- Oracle Private Cloud
- VMware ESXi versions 5.0, 5.5, 6.0, 6.5, 6.7, and 7.0

## Feature support

The following table lists FortiAnalyzer feature support for log devices.

Platform	Log View	FortiView	Event Management	Reports
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓
FortiADC	✓		✓	
FortiAnalyzer	✓		✓	
FortiAuthenticator	✓			

Platform	Log View	FortiView	Event Management	Reports
FortiCache	✓		✓	✓
FortiClient registered to FortiGate	✓	✓		✓
FortiClient registered to FortiClient EMS	✓	✓		✓
FortiDDoS	✓	✓	✓	✓
FortiMail	✓		✓	✓
FortiManager	✓		✓	
FortiProxy	✓		✓	✓
FortiSandbox	✓		✓	✓
FortiWeb	✓		✓	✓
Syslog	✓		✓	✓

## Language support

The following table lists FortiAnalyzer language support information.

Language	GUI	Reports
English	✓	✓
Chinese (Simplified)	✓	✓
Chinese (Traditional)	✓	✓
French		✓
Hebrew		✓
Hungarian		✓
Japanese	✓	✓
Korean	✓	✓
Portuguese		✓
Russian		✓
Spanish		✓

To change the FortiAnalyzer language setting, go to *System Settings > Admin > Admin Settings*, in *Administrative Settings > Language* select the desired language from the drop-down list. The default value is *Auto Detect*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can create your own language translation files for these languages by exporting a predefined language from FortiAnalyzer, modifying the text to a different language, saving the file as a different language name, and then importing the file into FortiAnalyzer. For more information, see the *FortiAnalyzer Administration Guide*.

## Supported models

This section identifies which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch, FortiWeb, FortiCache, and FortiProxy models and firmware versions can send logs to a FortiAnalyzer appliance running version 7.0.0. Please ensure that the log devices are supported before completing the upgrade.



Software license activated LENC devices are supported, if their platforms are in the supported models list. For example, support of FG-3200D indicates support of FG-3200D-LENC.

---

This section contains the following topics:

- [FortiGate models on page 21](#)
- [FortiCarrier models on page 25](#)
- [FortiADC models on page 26](#)
- [FortiAnalyzer models on page 27](#)
- [FortiAuthenticator models on page 28](#)
- [FortiCache models on page 28](#)
- [FortiDDoS models on page 28](#)
- [FortiDeceptor models on page 28](#)
- [FortiMail models on page 28](#)
- [FortiNAC models on page 29](#)
- [FortiProxy models on page 29](#)
- [FortiSandbox models on page 29](#)
- [FortiSwitch ATCA models on page 30](#)
- [FortiWeb models on page 30](#)

## FortiGate models

Model	Firmware Version
<b>FortiGate:</b> FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60EDSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate80E-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate301E, FortiGate-400D, FortiGate-400E, FortiGate-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2200E, FortiGate2201E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate3960E, FortiGate-3980E <b>FortiGate 5000 Series:</b> FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 <b>FortiGate DC:</b> FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC <b>FortiWiFi:</b> FortiWiFi-40F, FortiWiFi-40F-3G4G, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-60F, FortiWiFi-61E, FortiWiFi-61F <b>FortiGate VM:</b> FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-AZURE, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGateVM64-Xen, FortiGate-VMX-Service-Manager, FortiGate-VM64-IBM <b>FortiOS:</b> FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen <b>FortiGateRugged:</b> FortiGateRugged-60F, FortiGateRugged-60F-3G4G	7.0
<b>FortiGate:</b> FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80E, FortiGate-80E-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-90E, FortiGate-91E, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-400E, FortiGate-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3301E, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E <b>FortiGate 5000 Series:</b> FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1	6.4

Model	Firmware Version
<b>FortiGate DC:</b> FortiGate-800D-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC <b>FortiGate Hardware Low Encryption:</b> FortiGate-100D-LENC <b>FortiWiFi:</b> FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-61E, FortiWiFi-60F, FortiWiFi-61F <b>FortiGate VM:</b> FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-AZURE, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager, FortiGate-VM64-IBM <b>FortiOS:</b> FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen <b>FortiGateRugged:</b> FortiGateRugged-60F, FortiGateRugged-60F-3G4G	
<b>FortiGate:</b> FortiGate-30E, FortiGate-30E-3G4G-INTL, FortiGate-30E-3G4G-NAM, FortiGate-40F, FortiGate-40F-3G4G, FortiGate-50E, FortiGate-51E, FortiGate-52E, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-80D, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-90E, FortiGate-91E, FortiGate-92D, FortiGate-100D, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140D, FortiGate-140D-POE, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-400E, FortiGate-401E, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-601E, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3301E, FortiGate-3960E, FortiGate-3980E, FortiGate-1800F, FortiGate-1801F, FortiGate-4200F, FortiGate-4201F <b>FortiGate 5000 Series:</b> FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 <b>FortiGate DC:</b> FortiGate-80C-DC, FortiGate-600C-DC, FortiGate-800C-DC, FortiGate-800D-DC, FortiGate-1000C-DC, FortiGate-1500D-DC, FortiGate-3000D-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3240C-DC, FortiGate-3600C-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-DC, FortiGate-3980E-DC <b>FortiGate Hardware Low Encryption:</b> FortiGate-80C-LENC, FortiGate-600C-LENC, FortiGate-1000C-LENC <b>FortiWiFi:</b> FortiWiFi-30D, FortiWiFi-30D-POE, FortiWiFi-30E, FortiWiFi-30E-3G4G-INTL, FortiWiFi-30E-3G4G-NAM, FortiWiFi-50E, FortiWiFi-50E-2R, FortiWiFi-51E, FortiWiFi-60E, FortiWiFi-60E-DSL, FortiWiFi-60E-DSLJ, FortiWiFi-61E, FortiWiFi-60F, FortiWiFi-61F, FortiWiFi-80CM, FortiWiFi-81CM	6.2

Model	Firmware Version
<b>FortiGate-VM:</b> FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-ALIONDEMAND, FortiGate-VM64-AWS, FortiGate-VM64-AWSONDEMAND, FortiGate-VM64-AZUREONDEMAND, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-GCPONDEMAND, FortiGate-VM64-HV, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-Xen, FortiGate-VMX-Service-Manager <b>FortiGate Rugged:</b> FortiGateRugged-30D, FortiGateRugged-30D-ADSL-A, FortiGateRugged-35D, FortiGateRugged-60F, FortiGateRugged-60F-3G4G <b>FortiOS:</b> FortiOS-VM64, FortiOS-VM64-HV, FortiOS-VM64-KVM, FortiOS-VM64-Xen	
<b>FortiGate:</b> FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-GBL, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-40F, FG-40F-3G4G, FG-60F, FG-61F, FG-61E, FG-70D, FG-70D-POE, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-100F, FG-101F, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240-POE, FG-280D-POE, FG300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600D, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FortiGate-1800F, FortiGate-1801F, FG-2000E, FortiGate-2200E, FortiGate-2201E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301EFG-3600C, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FortiGate-3301E, FG-3960E, FG-3980E <b>FortiGate 5000 Series:</b> FG-5001D, FG-5001E, FG-5001E1 <b>FortiGate DC:</b> FG1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC <b>FortiGate Hardware Low Encryption:</b> FG-100D-LENC, FG-600C-LENC <b>Note:</b> All license-based LENC is supported based on the FortiGate support list. <b>FortiWiFi:</b> FWF-30D, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-61E, FortiWiFi-60F, FortiWiFi-61F, FWF-90D, FWF-90D-POE, FWF-92D <b>FortiGate VM:</b> FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZUREONDEMAND, FG-VM64-Azure, FG-VM64-GCP, VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM, FOS-VM64-Xen <b>FortiGate Rugged:</b> FGR-30D, FGR-35D, FGR-60D, FGR-90D	6.0
<b>FortiGate:</b> FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-DSLJ, FG-60E-POE, FG-60E-DSL, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100F, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240-POE, FG-280D-POE, FG-300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E	5.6

Model	Firmware Version
<b>FortiGate 5000 Series:</b> FG-5001C, FG-5001D, FG-5001E, FG-5001E1 <b>FortiGate 6000 Series:</b> FG-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F <b>FortiGate 7000 Series:</b> FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC <b>FortiGate DC:</b> FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG-1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC, FG-7060E-8-DC <b>FortiGate Hardware Low Encryption:</b> FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC <b>Note:</b> All license-based LENC is supported based on the FortiGate support list. <b>FortiWiFi:</b> FWF-30D, FWF-30D-POE, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FW-60E-DSL, FW-60E-DSLJ, FWF-60D-POE, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D <b>FortiGate VM:</b> FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-Azure, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOSVM64, FOSVM64-KVM, FOS-VM64-Xen <b>FortiGate Rugged:</b> FGR-30D, FGR-35D, FGR-60D, FGR-90D	
<b>FortiGate:</b> FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-DSL, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100F, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-200E, FG-201E, FGT-300D, FGT-300E, FGT-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E, FG-2000E, FG-2500E <b>FortiGate 5000 Series:</b> FG-5001C, FG-5001D, FG-5001E, FG-5001E1 <b>FortiGate 6000 Series:</b> FG-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F <b>FortiGate 7000 Series:</b> FG-7030E-Q, FG-7030E-S, FG-7040E-1, FG-7040E-2, FG-7040E-3, FG-7040E-4, FG-7040E-5, FG-7040E-6, FG-7040E-8, FG-7040E-8-DC, FG-7060E-1, FG-7060E-2, FG-7060E-3, FG-7060E-4, FG-7060E-5, FG-7060E-6, FG-7060E-8 (Update only) FortiGate 7000 series: FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC <b>FortiGate DC:</b> FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG-1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815DC, FG-7060E-8-DC <b>FortiGate Hardware Low Encryption:</b> FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC <b>Note:</b> All license-based LENC is supported based on the FortiGate support list. <b>FortiWiFi:</b> FWF-30D, FWF-30D-POE, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E-DSL, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D	5.4



Model	Firmware Version
<b>FortiGate VM:</b> FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM <b>FortiGate Rugged:</b> FGR-30D, FGR-30D-ADSL-A, FGR-35D, FGR-60D, FGR-90D	

## FortiCarrier models

Model	Firmware Version
<b>FortiCarrier:</b> FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 <b>FortiCarrier-DC:</b> FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC <b>FortiCarrier-VM:</b> FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	
<b>FortiCarrier:</b> FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3400E, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 <b>FortiCarrier-DC:</b> FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC <b>FortiCarrier-VM:</b> FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	
<b>FortiCarrier:</b> FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 <b>FortiCarrier-DC:</b> FortiCarrier-3000D-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC <b>FortiCarrier-VM:</b> FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	

Model	Firmware Version
<b>FortiCarrier:</b> FGT-3000D, FGT-3100D, FGT-3200D, FGT-3700D, FGT-3800D, FGT-3810D, FGT-3960E, FGT-3980E, FGT-5001D, FGT-5001E <b>FortiGate 6000 series:</b> FG-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F <b>FortiGate 7000 series:</b> FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC <b>FortiCarrier-DC:</b> FGT-3000D-DC, FGT-3100D-DC, FGT-3200D-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FGT-3960E-DC, FGT-3980E-DC <b>FortiCarrier-VM:</b> FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-Azure, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-Xen	6.0
<b>FortiCarrier:</b> FGT-3000D, FGT-3100D, FGT-3200D, FGT-3240C, FGT-3600C, FGT-3700D, FGT-3700DX, FGT-3800D, FGT-3810D, FGT-3960E, FGT-3980E, FGT-5001C, FGT-5001D, FGT-5001E <b>FortiCarrier 6000 Series:</b> FG-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F <b>FortiCarrier 7000 Series:</b> FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC <b>FortiCarrier-DC:</b> FGT-3000D-DC, FGT-3100D-DC, FGT-3200D-DC, FGT-3240C-DC, FGT-3600C-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FGT-3960E-DC, FGT-3980E-DC, FGT-7060E-8-DC <b>FortiCarrier-VM:</b> FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWS-AWSONDEMAND, FG-VM64-Azure, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-Xen	5.6
<b>FortiCarrier:</b> FGT-3000D, FGT-3100D, FGT-3200D, FGT-3240C, FGT-3600C, FG-3600E, FGT-3700D, FGT-3700DX, FGT-3800D, FGT-3810D, FGT-5001C, FGT-5001D, FGT-7030E, FGT-7040E <b>FortiCarrier 6000 Series:</b> FG-6000F, FG-6300F, FG-6301F, FG-6500F, FG-6501F <b>FortiCarrier 7000 Series:</b> FG-7030E, FG-7040E, FG-7060E, FG-7060E-8-DC <b>FortiCarrier-DC:</b> FGT-3000D-DC, FGT-3100D-DC, FGT-3200D-DC, FGT-3240C-DC, FGT-3600C-DC, FGT-3700D-DC, FGT-3800D-DC, FGT-3810D-DC, FGT-7060E-8-DC <b>FortiCarrier-VM:</b> FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWS-AWSONDEMAND, FG-VM64-Azure, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-Xen	5.4

## FortiADC models

Model	Firmware Version
FortiADC-100F, FortiADC-200D, FortiADC-200F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-4000D, FortiADC-4000F, FortiADC-5000F, FortiADC-VM	6.0
FortiADC-100F, FortiADC-200D, FortiADC-200F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-4000D, FortiADC-4000F, FortiADC-5000F, FortiADC-VM	5.4

## FortiAnalyzer models

Model	Firmware Version
<b>FortiAnalyzer:</b> FortiAnalyzer-150G, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3900E <b>FortiAnalyzer VM:</b> FortiAnalyzer-VM64, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	7.0
<b>FortiAnalyzer:</b> FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-1000E, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3900E <b>FortiAnalyzer VM:</b> FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-ALI-OnDemand, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWSOnDemand, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-GCP-OnDemand, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-KVM-CLOUD, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	6.4
<b>FortiAnalyzer:</b> FAZ-200F, FAZ-300F, FAZ-400E, FAZ-800F, FAZ-1000E, FAZ-2000E, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3700F and FAZ-3900E. <b>FortiAnalyzer VM:</b> FAZ-VM64, FAZ-VM64-Ali, FAZ-VM64-AWS, FAZ-VM64-AWS-OnDemand, FAZ-VM64-Azure, FAZ-VM64-GCP, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-OPC, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	6.2
<b>FortiAnalyzer:</b> FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E. <b>FortiAnalyzer VM:</b> FAZ-VM64, FAZ-VM64-AWS, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	6.0
<b>FortiAnalyzer:</b> FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E. <b>FortiAnalyzer VM:</b> FAZ-VM64, FAZ-VM64-AWS, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	5.6
<b>FortiAnalyzer:</b> FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, and FAZ-4000B. <b>FortiAnalyzer VM:</b> FAZ-VM64, FMG-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-XEN (Citrix XenServer and Open Source Xen), FAZ-VM64-KVM, and FAZ-VM64-AWS.	5.4

## FortiAuthenticator models

Model	Firmware Version
<b>FortiAuthenticator:</b> FAC-200D, FAC-200E, FAC-400C, FAC-400E, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000B, FAC-3000D, FAC-3000E <b>FortiAuthenticator VM:</b> FAC-VM	4.3, 5.0-5.5, 6.0

## FortiCache models

Model	Firmware Version
<b>FortiCache:</b> FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3000E, FCH-3900E <b>FortiCache VM:</b> FCH-VM64, FCH-KVM	4.0, 4.1, 4.2

## FortiDDoS models

Model	Firmware Version
<b>FortiDDoS:</b> FortiDDoS-200B, FortiDDoS-400B, FortiDDoS-600B, FortiDDoS-800B, FortiDDoS-900B, FortiDDoS-1000B, FortiDDoS-1200B, FortiDDoS-1500E, FortiDDoS-2000B, FortiDDoS-2000E	5.2, 5.3
<b>FortiDDoS:</b> FI-200B, FI-400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-1500B, FI-2000B, FI-2000E	5.1
<b>FortiDDoS:</b> FI-1500E, FI-2000E	5.0
<b>FortiDDoS:</b> FI-200B, FI-400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-2000B, FI-3000B	4.2, 4.3, 4.4, 4.5, 4.7

## FortiDeceptor models

Model	Firmware Version
FortiDeceptor-1000F, FortiDeceptor-VM	3.1

## FortiMail models

Model	Firmware Version
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-400E, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM, FML-60D, FML-200D, FML-1000D, FML-3000D, FML-200E, FML-400E, FML-2000E, FML-3000E, FML-3200E, FML-200F, FML-400F, FML-900F	6.4

Model	Firmware Version
<b>FortiMail VM:</b> FE-VM64, FE-VM64-HV, FE-VM64-XEN	
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-400E, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM, FML-60D, FML-200D, FML-1000D, FML-3000D, FML-200E, FML-400E, FML-2000E, FML-3000E, FML-3200E, FML-200F, FML-400F, FML-900F <b>FortiMail VM:</b> FE-VM64, FE-VM64-HV, FE-VM64-XEN	6.2
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-400E, FE-1000D, FE-2000E, FE-3000D, FE-3000E, FE-3200E, FE-VM, FML-200F, FML-400F, FML-900F	6.0
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000E, FE-3200E <b>FortiMail Low Encryption:</b> FE-3000C-LENC	5.4
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000D, FE-3000E, FE-3200E, FE-5002B <b>FortiMail Low Encryption:</b> FE-3000C-LENC <b>FortiMail VM:</b> FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.3

## FortiNAC models

Model	Firmware Version
FortiNAC-500, FortiNAC-600, FortiNAC-700, FortiNAC-C-1000C, FortiNAC-C-2000C, FortiNAC-C-VM, FortiNAC-CA-VM, FortiNAC-M-VM, FortiNAC-Manager-550	8.7
FortiNAC-500, FortiNAC-600, FortiNAC-700, FortiNAC-C-1000C, FortiNAC-C-2000C, FortiNAC-C-VM, FortiNAC-CA-VM, FortiNAC-M-VM, FortiNAC-Manager-550	8.6
FortiNAC-500, FortiNAC-600, FortiNAC-700, FortiNAC-C-1000C, FortiNAC-C-2000C, FortiNAC-C-VM, FortiNAC-CA-VM, FortiNAC-M-VM, FortiNAC-Manager-550	8.5

## FortiProxy models

Model	Firmware Version
<b>FortiProxy:</b> FPX-400E, FPX-2000E, FPX-4000E <b>FortiProxy VM:</b> FPX-KVM, FPX-VM64	1.0/1.1

## FortiSandbox models

Model	Firmware Version
<b>FortiSandbox:</b> FSA-500F, FSA-1000F, FSA-2000E, FSA-3000E <b>FortiSandbox-VM:</b> FSA-AWS, FSA-VM	4.0

Model	Firmware Version
<b>FortiSandbox:</b> FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D <b>FortiSandbox-VM:</b> FSA-AWS, FSA-VM	3.2
<b>FortiSandbox:</b> FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D <b>FortiSandbox-VM:</b> FSA-AWS, FSA-VM	3.1
<b>FortiSandbox:</b> FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D <b>FortiSandbox VM:</b> FSA-AWS, FSA-VM	3.0
<b>FortiSandbox:</b> FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D <b>FortiSandbox VM:</b> FSA-KVM, FSA-VM	2.5.2
<b>FortiSandbox:</b> FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D <b>FortiSandbox VM:</b> FSA-VM	2.4.1 2.3.3
<b>FortiSandbox:</b> FSA-1000D, FSA-3000D, FSA-3500D <b>FortiSandbox VM:</b> FSA-VM	2.2.0

## FortiSwitch ATCA models

Model	Firmware Version
<b>FortiController:</b> FTCL-5103B, FTCL-5902D, FTCL-5903C, FTCL-59	5.2.0
<b>FortiSwitch-ATCA:</b> FS-5003A, FS-5003B <b>FortiController:</b> FTCL-5103B, FTCL-5903C, FTCL-5913C	5.0.0

## FortiWeb models

Model	Firmware Version
<b>FortiWeb:</b> FortiWeb-400C, FortiWeb-3000C, FortiWeb-4000C, FortiWeb-3000CFSX, FortiWeb-100D, FortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-3000D, FortiWeb-4000D, FortiWeb-3000DFSX, FortiWeb-400E, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000E <b>FortiWeb VM:</b> FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	6.4
<b>FortiWeb:</b> FortiWeb-400C, FortiWeb-3000C, FortiWeb-4000C, FortiWeb-3000CFSX, FortiWeb-100D, FortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-3000D, FortiWeb-4000D, FortiWeb-3000DFSX, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000E	6.3

Model	Firmware Version
<b>FortiWeb VM:</b> FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	
<b>FortiWeb:</b> FortiWeb-400C, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-100D, FortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E	6.2
<b>FortiWeb VM:</b> FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	
<b>FortiWeb:</b> FortiWeb-400C, FortiWeb-3000C, FortiWeb-4000C, FortiWeb-3000CFSX, FortiWeb-100D, FortiWeb-400D, FortiWeb-600D, FortiWeb-1000D, FortiWeb-3000D, FortiWeb-4000D, FortiWeb-3000DFSX, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-3000E, FortiWeb-3010E, FortiWeb-4000E	6.1
<b>FortiWeb VM:</b> FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-Docker, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XenServer	
<b>FortiWeb:</b> FWB-400C, FWB-100D, FWB-400D, FWB-600D, FWB-1000D, FWB-1000E, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E	6.0.1
<b>FortiWeb VM:</b> FWB-VM, FWB-HYPERV, FWB-XENOPEN, FWB-XENSERVER	
<b>FortiWeb:</b> FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D	5.9.1
<b>FortiWeb VM:</b> FWB-Azure, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	
<b>FortiWeb:</b> FWB-1000C, FWB-1000D, FWB-1000E, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D	5.8.6
<b>FortiWeb VM:</b> FWB-Azure, FWB-Azure-Ondemand, FWB-CMINTF, FWB-HYPERV, FWB-KVM, FWB-KVM-PAYG, FWB-VM, FWB-VM-PAYG, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	
<b>FortiWeb:</b> FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D	5.7.2
<b>FortiWeb VM:</b> FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-OS1, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	
<b>FortiWeb:</b> FWB-1000C, FWB-1000D, FWB-100D, FWB-2000E, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E, FWB-400C, FWB-400D, FWB-600D	5.6.1
<b>FortiWeb VM:</b> FWB-Azure, FWB-HYPERV, FWB-KVM, FWB-VM, FWB-XENAWS, FWB-XENAWS-Ondemand, FWB-XENOPEN	

Model	Firmware Version
<b>FortiWeb:</b> FWB-100D, FWB-400C, FWB-400D, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E	5.5.6
<b>FortiWeb VM:</b> FWB-VM-64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV, FWB-KVM, FWB-AZURE	
<b>FortiWeb:</b> FWB-100D, FWB-400C, FWB-1000C, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E	5.4.1
<b>FortiWeb VM:</b> FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV	



# Resolved Issues

The following issues have been fixed in FortiAnalyzer version 7.0.0. For inquiries about a particular bug, please contact [Customer Service & Support](#).

## Device Manager

Bug ID	Description
521774	The <i>Add</i> and <i>Delete</i> function for unregistered devices are greyed out even when the root ADOM is locked.
523721	FortiAnalyzer should support FortiADC device type.
622649	When a FortiGate HA device is deleted, their log files are not deleted.
696853	When manually adding a device in FortiNAC ADOM, version v8.8 is not listed in the version option.

## Fabric View

Bug ID	Description
554251	A user may not be able to see the fabric topology of devices in the user's assigned ADOM.

## FortiSOC

Bug ID	Description
656293	FortiAnalyzer should automatically retrieve all software inventory after EMS connector is created.

## FortiView

Bug ID	Description
668494	FortiView may not apply filter correctly for many of the entries.

Bug ID	Description
668922	Selecting <i>FortiGate</i> in <i>FortiView Traffic</i> logs returns <i>Invalid params: Cannot find device XXX under adom XXX</i> .
670844	<i>Resources Usage Peak</i> shows higher bandwidth than real usage.
671620	FortiAnalyzer <i>SD-WAN View</i> is not showing correct SLA output and cannot filter on specific SLA.
673477	FortiView map may fail to display traffic.
674461	Within FortiView VPN logs, the <i>Country Flags</i> may be incorrect.
678250	FortiView may show error when drill-down IOC rescan details.
682485	Policy hit count may be shown as zero while there is traffic.
682657	FortiView may not be refreshed correctly after switching between ADOMs.
684131	<i>Top Sources</i> response may be slow when filtering by <i>Policy ID</i> .
684193	Secure SD-WAN Monitor should not send a request when device list fails to load.
690895	<i>FortiView &gt; Monitors &gt; Secure SD-WAN Monitor &gt; SD-WAN Rules Utilization</i> widget may show <i>No Data</i> for some FortiGates.
691570	FortiAnalyzer may not be able to cancel <i>IOC re-scan</i> task.
692464	FortiAnalyzer may prompt XSS erro while retrieving IPS error log details.
692852	After upgrade, the Secure <i>SD-WAN Monitor</i> may show <i>No Data</i> for <i>Performance</i> , <i>Jitter</i> , <i>Latency</i> , or <i>Packet loss</i> widget.
702268	Loading the <i>FortiView</i> page may be very slow when the <i>Source</i> is set as <i>FortiAnalyzer</i> when accessing it from FortiGate.

## Log View

Bug ID	Description
522202	FortiAnalyzer may not able to accept syslog from FortiVoice.
591272	Downloaded Logs files from <i>Log View</i> or browse are not in the correct CSV format.
600083	<i>Endpoint Identification</i> should always show the same user tied to the same session.
625306	Hiding column(s) in Log view may cause filters to reference to incorrect column.
638388	When two filters are defined and the first filter is removed, clicking on the remaining filter may incorrectly reference a removed filter.
639228	FortiAnalyzer needs to synchronize FortiClient 6.4.1 new log format changes for Value of <i>Type</i> , <i>Sub-type</i> , and <i>Event Type</i> .
643858	Actual analytics logs do not match what is observed in log view.

Bug ID	Description
652076	<i>Log view may take a long time to load with Custom Time Period.</i>
672350	FortiAnalyzer should be able to view the space in between the user name on <i>Log View &gt; Event &gt; VPN &gt; User</i> column.
672763	<i>Level</i> Column is empty on GUI when switching to Real-time Log on a FortiAnalyzer ADOM.
690922	The event logs filter should only display logs from its own VDOM.

## Others

Bug ID	Description
578907	The <i>exec log-aggregate all</i> should aggregate all log files without any error.
595696	The change of value for <i>system.global.enc-algorithm</i> is not applied to <i>oftpd</i> until a reboot.
610161	FortiAnalyzer may unexpectedly set <i>Don't Fragment</i> flag with jumbo frame related packets in OFTP communications and in log forwarding.
621473	FortiSOC is missing in cloud-based VMs.
653646	When formatting disk, database server may fail to shut down.
656370	FortiAnalyzer SCP backup cannot be stopped.
665273	The <i>diagnose system ntp status</i> command may return error <i>/bin/ntpq: read: Connection refused</i> .
666940	<i>ADOM Mode</i> Information has outdated wording about <i>Reduced operation</i> .
673224	The <i>sqllogd</i> may keep crashing after upgrading FAZ-3700F secondary unit.
675273	FortiAnalyzer to add <i>SFTP</i> and port support for all export commands.
675930	When calling an API, FortiAnalyzer may not update the progress with correct percentage.
676103	<i>Webhook Fabric Connector</i> sends the wrong <i>Sever Name Indication (SNI)</i> in the TLSv1.2 Client Hello.
677494	FortiAnalyzer may return SQL query error when creating temporary table <i>blk1st</i> during <i>ioc-rescan</i> . <b>Workaround:</b> Please set <i>ioc-rescan</i> days to less than database compression days.
678200	FortiAnalyzer may stop inserting logs using high CPU usage.
681884	HA synchronization may stall at a random percentage.
682997	FortiAnalyzer may show <i>fmgd</i> crash during boot up after upgrade.
687809	Log insert lag time may go above 5 hours on a properly sized FortiAnalyzer.
693161	When frequently accessing different pages, FortiAnalyzer's GUI may become sluggish and pages may not transition.

Bug ID	Description
696211	Secondary FortiAnalyzer accepts FTP connections after disabling FortiRecorder.
697654	FortiAnalyzer may return duplicated data within log view JSON response.
702140	The <code>disable-module</code> setting resets to default after reboot.

## Reports

Bug ID	Description
547496	FortiAnalyzer generates a report for selected device with outputs for all devices.
624911	FortiAnalyzer may not be able to generate the <i>SaaS Application Usage Report with Obfuscate User</i> feature.
647868	After upgrade, all default reports and event handler list are lost.
662442	FortiAnalyzer should show <i>report</i> , <i>template</i> , <i>chart library</i> , and <i>dataset</i> under report section.
677060	Default <i>Reports</i> , <i>Templates</i> , <i>Chart Library</i> , <i>Macro Library</i> , or <i>Datasets</i> are missing on newly created ADOMs.
677109	Graphics may not be complete for <i>FortiGate Performance Statistics Report</i> .
695960	When accessing <i>Throughout Utilization Billing Report</i> , FortiAnalyzer may show a vertical line on the <i>Interface Throughout Distribution</i> chart when there is no interface data available.
704544	Application icons may not be displayed in report.

## System Settings

Bug ID	Description
560895	FortiAnalyzer should separate the Admin profile setting for <i>Log</i> and <i>SoC</i> views.
580629	Chromebooks are unable to log to FortiAnalyzer if the admin has trusted hosts configured.
627683	The <i>GB/day</i> displayed in <i>License Widget</i> may not be correct.
631709	Email should be sent successfully from FortiAnalyzer with SMTPS TCP/465.
660798	<i>Device Log Settings &gt; Upload to FTP</i> may not working correctly in <i>collector-analyzer</i> setup.
668067	NTPv3 enabled with authentication is not sending NTP client request with hardware platforms.
672633	FortiAnalyzer HA primary unit may stop log insertion when there is <i>postgres UPDATE</i> on <i>IOC</i> .
681321	Avatar may always synchronizing resulting in <i>init sync</i> cannot be finished.

Bug ID	Description
681622	SMTP server password should not be limited to 63 characters.
689824	After upgrade, log filter setting may set to <i>Equal to</i> for log forwarding.
691798	The secondary unit in FortiAnalyzer HA cluster may report <i>HA cluster config-sync DOWN, cause=keepalive failure</i> every couple of days.
708047	There may be multiple <code>devid</code> , <code>devname</code> , or <code>tz</code> columns when logs are forwarded in syslog.

# Known Issues

The following issues have been identified in FortiAnalyzer version 7.0.0. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

## Device Manager

Bug ID	Description
639479	FortiGate v6.0 with sub-ca certificate may not be able to establish <i>oftp</i> connection with FortiAnalyzer without sub-ca certificate.

## Event Management

Bug ID	Description
691220	Event handler may not be triggered correctly when there is more than one match.

## FortiView

Bug ID	Description
579910	SOC should show AP SSIDs and clients from Event Logs when the <i>Service Profile</i> is in <i>Bridge</i> mode.
616675	Bandwidth may not match between FortiAnalyzer and FortiGate.
621453	FortiGate cannot get FortiClient's vulnerability detail information from FortiAnalyzer.
626530	<i>Bytes Sent/Received</i> should match between <i>Top Destinations</i> and <i>Policy Hit</i> charts under <i>FortiView</i> when filtered by the same policy ID.
640553	FortiView monitor <i>WiFi</i> widget is not showing <i>Bridged SSID</i> information.
641596	FortiAnalyzer may show <i>No Data</i> in <i>User Vulnerabilities Summary</i> widget.
642837	If Sandbox detection only supports FortiGate in Fabric ADOM, there should be an indication on GUI.
663930	Ports status is not correct in <i>Secure SD-WAN</i> monitor and <i>SD-WAN Performance</i> status.
667076	FortiView Top Cloud Users may show "no entry found" message but there is a session graph

Bug ID	Description
	shown.
683525	The return lines may be incorrect after adding filters to <i>Top Website Categories</i> .
683580	The <i>Not</i> operation may not work for advanced filter.
685452	The <i>Not</i> filter filter may not work properly.
688141	FortiAnalyzer should be able to apply multiple negative filters from the same type.
707480	Top Threats (FortiClient) may only display Threat level <i>LOW</i> and <i>Allowed</i> incidents.
708006	<i>Monitors &gt; Endpoints</i> does not show all FortiClient endpoints in the logs.
711810	<i>SSL Dialup IPSec</i> connection count may not match with connection list.
713083	FortiAnalyzer may show a <i>No Data</i> message for the <i>Worldwide Threat Prevalence</i> chart.

## Log View

Bug ID	Description
608139	Opening compressed FortiClient traffic file on FortiAnalyzer may cause other compressed FortiClient traffic logs to fail to open.
633393	Some IPS archive files do not contain whole <i>Attack Context</i> but only contain <i>BODY</i> that is part of <i>Attack Context</i> .
635598	FortiAnalyzer may not display Traffic Logs in Log View and return <i>Web Server Error 500</i> .
641013	After creating an ADOM for FortiMail, the ADOM is not visible on GUI and mail domain logs are not going to the default FortiMail ADOM.
653765	Some log files under <i>Log Browse</i> may contain a mix of event and traffic messages.
661094	In <i>Log View</i> , importing log may fail.
674027	Filtering FortiClient event logs with wildcard <i>UID</i> filter returns no data.
686924	Downloading CSV file contains <i>tunnel-up</i> and <i>tunnel-down</i> VPN logs from other devices that belong to different ADOMs.
704206	When filtering with <i>Action</i> and <i>Source IP</i> under the <i>Traffic</i> menu, the filter output may be incorrect with the combination of smart action with any other field.
711711	Log filter may show unfiltered values.

## Others

Bug ID	Description
584105	The <code>/drive0/private/restapi/sync/fgt_intf_stat</code> location may use too many inodes.
616355	FortiGate may display "SSL error" or "OFTP error" when testing connectivity with FortiAnalyzer.
625343	FortiAnalyzer may consume high on I/O resources every hour by fazwatch.
632971	FortiAnalyzer should have the ability to query CPU utilization on individual CPU core.
700562	When creating a system admin user using JSON API, FortiAnalyzer may return an error: <i>The data is invalid for selected url.</i>
701753	SIEM database should be trimmed at the same time when quota enforcement occurs.
724625	Upgrade from 6.4.6 to 7.0.0 will result in all configuration being lost.

## Reports

Bug ID	Description
628823	FortiAnalyzer is not generating all local Event logs for reports.
653207	FortiAnalyzer may have incorrect dataset queries without considering the <i>direction</i> field.
677090	Report filter may not work with <i>devname</i> .
683668	The FortiClient report is always empty after enabling device filter.
692097	Report sub-charts may not work after upgrade.

## System Settings

Bug ID	Description
630654	Imported logs may not sync to slave.
634253	ADOMs may disappear randomly from ADOM configuration while editing it.
638380	FortiAnalyzer may accept invalid dashboard configurations which may break some widgets.
666767	When log forwarding is enabled, there may be <i>logfwd</i> crashes with high log rate.
669402	FortiAnalyzer may not time out admin session after many hours.
673591	FortiAnalyzer may return error, <i>cfgerror:1</i> , when editing and saving an admin user.



# Appendix A - Default and maximum number of ADOMs supported

This section identifies the supported number of ADOMs for FortiAnalyzer hardware models and virtual machines.

See also the [FortiAnalyzer Data Sheet](#).

## Hardware models

FortiAnalyzer supports a default number of ADOMs based on hardware model.

Some hardware models support an ADOM subscription license. When you purchase an ADOM subscription license, you increase the number of supported ADOMs. For example, you can purchase an ADOM subscription license for the FAZ-3000G series, which allows you to use up to a maximum of 1200 ADOMs.

Other hardware models do not support the ADOM subscription license. For hardware models that do not support the ADOM subscription license, the default and maximum number of ADOMs is the same.

FortiAnalyzer Platform	Default number of ADOMs	Maximum number of ADOM
Desktop models	1	1
300F/400E Series and higher	25	25
800F/1000F Series	50	50
2000E Series	250	250
3000F Series	500	500
3000G Series	500	1200
3500F/3500G	500	500
3700F Series	1200	1200

## Virtual Machines

Five (5) ADOMs are included with FortiAnalyzer VM subscription licenses. Licenses are non-stackable. Additional ADOMs can be purchased with an ADOM subscription license.

FortiAnalyzer Platform	Default number of ADOMs
1 GB/Day < License <= 5 GB/Day	10

FortiAnalyzer Platform	Default number of ADOMs
5 GB/Day < License <= 25 GB/Day	25
25 GB/Day < License <= 100 GB/Day	50
100 GB/Day < License <= 500 GB/Day	250
500 GB/Day < License <= 1000 GB/Day	500
1000 GB/Day < License <= 5000 GB/Day	800
License > 5000 GB/Day	1200



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.